DOCUMENT RESUME

ED 235 530 CS 504 376

AUTHOR Wigand, Rolf T.; And Others
TITLE Transborder Data Flow, Informatics and National Policies: A Comparison among 22 Nations.
PUB DATE May 83
NOTE 44p.; Paper presented at the Annual Meeting of the International Communication Association (Dallas, TX, May 26-30, 1983).
PUB TYPE Speeches/Conference Papers (150) -- Information Analyses (070)

EDRS PRICE MF01/PC02 Plus Postage.
DESCRIPTORS Change Agents; Communication Research; Computers; Developing Nations; Foreign Policy; Futures (of Society); *Information Dissemination; *Information Networks; Information Utilization; *International Law; International Organizations; *International Relations; International Studies; *Technological Advancement; Telecommunications

ABSTRACT

The product of advanced information technology and digital transmission capabilities, transborder data flow (TDF)--the flow of information across national borders via computer and other electronic communications systems--has considerable political, social, economic, and legal implications. Important issues in TDF include (1) the regulation of telecommunication planning and development among various nations without stifling innovations; (2) the protection of personal privacy; (3) the impact of TDF on the cultural identity of information receiving nations; (4) the expatriation of national information; (5) the treatment of information as a commodity; (6) the impact of TDF on developing nations' balance of trade, employment, and infant information services; and (7) the restriction of competition and market entry of transnational corporations through such legislated and nonlegislated barriers as tariffs and prohibitive pricing. While current international legislation on TDF may appear excessive to those hoping to profit from expanding telecommunications systems, to people wanting to improve privacy protection or protect fledgling information economies, it seems minimal. Greater international cooperation is needed to balance the need for a free flow of information with other needs for personal and national protection and benefit. (MM)

****
* Reproductions supplied by EDRS are the best that can be made *
* from the original document. *
****

U.S. DEPARTMENT OF EDUCATION
NATIONAL INSTITUTE OF EDUCATION
EDUCATIONAL RESOURCES INFORMATION
CENTER (ERIC)
X This document has been reproduced as received from the person or organization originating it.
☐ Minor changes have been made to improve reproduction quality.
• Points of view or opinions stated in this document do not necessarily represent official NIE position or policy.

ED235530

TRANSBORDER DATA FLOW, INFORMATICS AND NATIONAL POLICIES:

A COMPARISON AMONG 22 NATIONS

Presented to the

International Communication Association
Annual Convention
Session on 'Technology and Information Flow'
Information Systems Division
May 28, 1983

"PERMISSION TO REPRODUCE THIS MATERIAL HAS BEEN GRANTED BY
Rolf T. Wigand
TO THE EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)."

Presented by:

Rolf T. Wigand, Ph.D.
Center for Public Affairs
Arizona State University
Tempe, AZ 85287

Carrie Shipley
Department of Communication Arts
Cornell University
Ithaca, New York 14853

Dwayne Shipley
Consultant
P.O. Box 6813
Ithaca, New York 14850

CS 504 376

TRANSBORDER DATA FLOW, INFORMATICS AND NATIONAL POLICIES:
A COMPARISON AMONG 22 NATIONS

Abstract

The term transborder data flow (TDF) includes a host of issues in the complex and far-reaching debate on the shape and regulation of the international information and communication system. The technology of sychronously orbiting communication satellites provides communication services at international levels with considerable ease. High quality communication links and channels have increased and their costs have decreased sharply. When these and other new telecommunication technologies are combined with computer chips in an international context, communication by data users becomes inexpensive, instantaneous and ubiquitous. Terminals in one nation can communicate with terminals in other nations or data bases virtually anywhere in the world. However, such developments have jeopardized national sovereignty and personal privacy protection.

In recent years the protection of privacy of individuals has become the focus of national and--to some extent--international legislative concerns. In turn, national legislation on privacy and access issues has created a fear of impediments to the free flow of data. Almost all Western countries are presently considering or have already enacted data protection laws. Although the laws are not specifically designed with regard to the data needs of social researchers, such regulations and policies affect the latter.

This paper identifies the key issues underlying the complex setting of transborder data flow. The authors collected data in over 22 countries that are currently considering or have already enacted regulation of transborder data flow for whatever reason. Most of these concerns are based on various legislative efforts of national governments to protect personal data within a nation's sovereign territory and to protect personal data transmitted abroad. The

currently prevailing situation in these 22 countries is described, presented in tabular format and analyzed. This discussion includes the general characteristics of national data protection, regulations concerning data collection, access to administrative and process-produced data for research purposes, and the preservation and access to archive data. It describes also the implementation of data-protection laws and practices of data protection at all levels of government. Reactions of nations and transnational corporations to these developments, e.g., the development of so-called data havens, are also described. In order to avoid unnecessary restrictions on transborder data flow and to facilitate solutions to worldwide problems of sovereignty and privacy, it will be imperative to develop and agree upon international standards of data flow and privacy protection. This paper describes the importance of monitoring and periodically evaluating the status and adequacy of transborder data flow and privacy legislation.

TRANSBORDER DATA FLOW, INFORMATICS AND NATIONAL POLICIES: A COMPARISON AMONG 22 NATIONS

Overview

During the last decade of transborder data flow (TDF) policy formation, international interest in TDF issues has run the gamut from personal privacy protection to freedom of information and rights of personal access to information. Now, however, primary focus seems to be shifting away from these issues in international arenas of discussion. Concern is rising about worldwide protectionism of fledgling information industries, vis-a-vis the domination of the international markets for these industries by major transnational corporations. Unfortunately, even while the focus is shifting, it is not yet entirely apparent how recent privacy legislation will affect international communication. But the need for or concern about information protectionism is already sponsoring further policy-formation, as many industrial and developing nations erect barriers to TDF, barriers that are being positioned via legislative and non-legislative (economic) means. Although much of the legislative action in the past did bear the title of privacy legislation, such action also may serve protectionist purposes, since actual effects of regulation on TDF are often the same as if trade restraint was intended (Donovan, 1981). Economic barriers are more complex and less easily identifiable than legislated barriers, nonetheless they also are restrictive.

What does this mean to vendors and clients or other users of international information networks and data bases? Significant effects are already manifest, although ramifications are complex, and the full impact on society may not be felt for years to come. But effects of TDF regulation can only be examined once background issues and underlying causes of the regulatory trend are fully understood. Therefore, the nature and scope of TDF regulation will be considered here in light of the direct influence of technical, social, economic,

and political/legal issues and circumstances. Subsequently, specific requirements of current TDF regulations and their effects on TDF users will be discussed.

Technical Considerations: Some Definitions and the Emergence of TDF Policy Concerns

It is almost a cliche today to state that we live in the Information Age. Numerous researchers have addressed this phenomenon. Among them, Marc Uri Porat in his landmark study, The Information Economy, recognized information as a basic resource of the post-industrial era. Porat defines information as "data that have been organized and communicated. The information activity includes all the resources consumed in producing, processing and distributing information goods and services" (Porat, 1977, p.2). Porat argued that, aside from the traditional three-sector approach (industry, service, agriculture) for analyzing the economy, a new fourth sector -- the information sector -- has emerged over the last twenty years. There is no question that during this time span a dramatic rise of the use and generation of information could be observed. Throughout the world, information is being treated more and more as a marketable commodity and resource.

With the advent of advanced technology and digital transmission capabilities, transborder data flow is a fairly recent phenomenon and debated issue with considerable political, social, economic and legal implications. The recent convergence of computer, information and telecommunications technology has brought about the coinage of the terms informatics or informatique, and telematics or telematique. Through this convergence and as information and data cross national boundaries, transborder data flow has become an international issue.

Transborder data flow may be defined as machine-readable data and information transmitted over transnational computer and other electronic communication systems for the purpose of storage, retrieval or processing. Data here are understood as basic symbols that can be

processed and stored in digital or analog symbols and can be processed or stored in computers. Information one may view here as a combination of data into messages readily understandable by human beings. The information transmitted is typically of a proprietary nature and, increasingly, is transmitted in an encoded fashion. The transmission of data involves point-to-point delivery of messages and may occur via electronic over-the-air or via electronic terrestrial networks, but may also be transmitted by non-electronic means via the manual transfer of magnetic tapes, discs, cards or other media. Messages and information diffused transnationally by mass media such as broadcasting are not discussed here.

Increases in transborder data flow today result, no doubt, mainly from electronic transmission replacing traditional use of media such as telex, telephone and the mail. Such transmissions require an appropriate computer and telecommunications infrastructure to exist in participating nations. This infrastructure may be designed and developed by the nation's government or it may be in private possession as is occasionally the case with transnational corporations. Some transnational corporations are independent and may not have to rely upon an existing infrastructure in a nation. The corporation may own its own facilities and transmission devices as is now achievable with satellite transmissions. Satellite set-ups or the use of dedicated transmission networks allow for increased information mobility, speed, accessibility, interactive capabilities, and lower costs (Wigand, 1982). Time, distance and location are no longer major concerns. Combining these assets gives transborder data flow a potency previously unparalleled in international communication activities.

It was not the newer technology alone that instituted transborder data flow as an issue and activity to be studied. Since the distribution and production of information goods and services started to cross national boundaries, numerous business activities over the last twenty years have been internationalized and final products may

be composed of parts produced and assembled on several continents. Numerous information-intensive industries such as banking, tourism, air transportation, geologic explorations and insurance are now operating on a world-wide, and more frequently, on-line basis.

A large number of data and information services are available to business and organizations on a time-share basis, and make many advanced computer and telecommunications technologies affordable. Since distance, time of day and the crossing of national boundaries are no longer an issue for today's advanced technology (Wigand, 1983c), it is quickly conceivable how the dissemination, collection, control and access of information to or from one country on an international basis can become a major policy issue.

The reader may consider the following situations: Burnham (1978) reports that when a fire alarm sounds in Malmo, Sweden, a fireman puts the address of the fire into a computer and gets back an immediate description of all the hazards in the area. The computer providing the information is located in Cleveland, Ohio. Similarly, Read (1977) reports that a number of Eastern European airlines, including Balkan Bulgarian, Czechoslovakian, Malev Hungarian, and LOT Polish Airlines belong to an international air carrier communication service that assists them in handling reservations. The organization to which they subscribe uses a Control Data computer in Atlanta, Georgia, to handle the reservations.

One can readily envision how just these two examples can trigger a heated debate on such issues as control of information, information-rich vs. information-poor countries, the growth of multinational organizations, the world information order and numerous other TDF policy issues. Some of the key issues surrounding the current debate over TDF are reviewed on the following pages.

Technical Considerations: Infrastructure

As already indicated, aside from computers, transborder data flow relies on an infrastructure through which data are channelled. A

given nation may provide such transmission possibilities through private or government-owned telephone networks, microwave networks or satellite receive and transmit facilities. Such networks and facilities may be integrated and the potential user has a choice of which network to use. In most countries, such networks are operated by the PTT, and they serve as common carriers. During the 1960s, organizations engaged in international telecommunications typically used standard telephone or telex service on a leased line or general public-access basis. A shift occurred, however, during the 1970s, i.e. organizations could purchase enhanced and dedicated network and computing services from such corporations (carriers) as Tymshare, General Electric and Control Data.

One such common carrier providing transnational services is Satellite Business Systems (SBS), a joint venture among IBM, and its subsidiaries COMSAT General Corporation and Aetna Life and Casualty Company. SBS utilizes communication satellites and provides its business customers worldwide integrated digital, encoded data, voice, facsimile and image transmission services to be used as an in-house, dedicated network. SBS's communication network is no longer dependent upon the services of the Bell telephone system, but rather links computers together via satellites at on-line speeds over long distances. The resulting high-speed service (at up to 6.3 megabits per second) is fast enough to transmit in one minute a file or data base that took an entire hour just ten years ago. One should envision that a one-billion byte file or eight billion bits, an amount of information of a magnitude that would have to be delivered by truck if it were printed on paper, could be distributed to one or numerous dispersed locations simultaneously anywhere in thirty minutes (Wigand, 1982).

Another type of carrier must be recognized: Value-added carriers, or a carrier's carrier, are carriers that lease time and lines from common carriers and may sell time and lines to other users of the network. Such value-added carriers make networks available on a fixed contract, time-share, cost-share, or subscription basis. Value-added

networks are essential for many users in transborder data flow since the quality of transmission lines is upgraded, usually dedicated, and this service implies a fast, highly reliable, flexible, and very cost-effective link for computer-based transmissions.

For transborder data flow purposes, the two most important privately-owned and truly intercontinental value-added networks are TELENET and TYMNET. The two most important public value-added networks are EURONET and the Nordic Public Data Network. The linking and integration of networks is becoming more observable. A prime example is the linkage between Western market-economy countries and Eastern European countries. The liaison function in this linkage is provided by the International Institute for Applied Systems Analysis (IIASA) in Laxenburg, Austria.

One can see readily that added linkages of networks with other networks enhance considerably the growth of an international telecommunication infrastructure for transborder data flow purposes. Numerous information and data providers, processors and researchers can take advantage of an international market with around-the-clock and on-line capabilities. Reports issued by the Organisation for Economic Co-Operation and Development (OECD) in Paris, as well as the United Nations Economic and Social Council, have estimated that the number of computer-readable, publicly-accessible reference data bases alone increased from over 300, with approximately 50 million records in 1974, to over 500, containing nearly 150 million records in 1979 (United Nations Centre on Transnational Corporations, 1981). One has to add about 150 numeric data bases to these reference data bases. More recent figures indicate even greater increases. According to one journal, "The number of on-line data bases publicly available is over 1,100 and this number is growing at about 20 percent a year" (Transnational Data Report, 1982a, p. 340). As can be imagined, a wide variety of information is available from these data bases: commodity trends, sales data, industry data, financial time series of firms; data on technology, licensing, patents; etc.

In Western Europe it is estimated that the number of network termination points will increase from 393,000 in 1979 to 1,620,000 in 1987. During the same time period, an increase is expected from 625,000 terminals to almost four million. These added capabilities will increase the volume of data transmissions in Western Europe alone from about 136 million in transactions in 1979 to nearly 800 million in 1987. During the same time frame, a rise from 10 to 15 percent is expected for international transactions (United Nations Centre for Transnational Corporations, 1981).

Technical Considerations: Harmonization

The European Community formulated a checklist of actions to respond to the growth of information and communications technologies in society. In the Commission of the European Communities' (Commission) report, "European Society Faced With the Challenge of New Information Technologies: A Community Response," a number of specific proposals were offered including, "use of the normative powers of the Community to create a homogeneous European public market for telematic equipment and services through Council decisions ..." (Commission, 1979, p. 6). One of the key methods that the European Community intends to employ is "standardization in order to harmonize the public markets in the fields of telecommunication and data processing" (Commission, 1979, p. 24).

The European Community appears committed to an aggressive course of action which could have disturbing ramifications for United States enterprises. On September 1, 1980 the Commission issued three additional reports (Commission, 1980). The first, "New Information Technologies: First Commission Report," notes that "it would not be appropriate to adopt a piecemeal approach whereby the Community framework would be selected whenever it was feasible from a political or technical angle; such a[n] approach would waste unnecessary time in a field where the pace of development is extremely fast." Rather, the Commission "recommends the adoption of an overall community strategy,"

the key elements of which are laid out in the report. In the two accompanying reports, one proposing regulations for telecommunications and the other regulations for microelectronics, the Commission puts regulatory flesh on the strategy outlines in the "First Report." The telecommunications recommendations are of particular interest to the United States Government and to U.S. based enterprises. The Commission seeks authority to oversee and implement "harmonisation" in telecommunications planning and development among member nations. It also urges the creation of a European-wide market, to benefit primarily European manufacturers and service suppliers. Standardization of hardware allows wider user access to more varieties of software and promotes easier interfacing for network integration. Too much control, however, can result in stifled innovation on the part of those competing to develop new technology.

Social TDF Issues: The Individual

Social issues and forces at the individual, cultural, national, and international levels of society are also major determinants of TDF regulation. At the individual's level, a growing concern is the computerized invasion of personal privacy. More and more restrictions are imposed upon computerized compilation and dissemination of personal data. As George Trubow (1981) indicates, "The rapid evolution of larger, cheaper and faster computer systems has increased dramatically the power of organizations and individuals to use or abuse information about others." When information was stored strictly in manual files and transmitted by less automated means, there was considerably less cause for concern. This concern was also evident when a majority of Americans polled in a Harris survey indicated that they "consider[ed] the present use of computers an actual threat to personal privacy." Those questioned also agreed (63%) that "if privacy is to be preserved, the use of computers must be sharply restricted in the future" (Trubow, 1981). Yet at the same time, individuals are increasing demands for home and office computers and

for use of telecommunications services. Similarly, in early 1983, after vehement discussions in the press and in the Lower House, the Federal Republic of Germany postponed the enactment of a proposed law that would have brought about West Germany's first nationwide census. These discussions were focused on privacy protection issues, even though West Germany has a national compulsory registration law. As a result, the first census is likely to occur not sooner than 1985 (Süddeutsche Zeitung, 1983, p. 23).

At the present time, a good number of countries have issued and enacted privacy protection and personal data laws. The Paris-based Organisation for Economic Co-Operation and Development (OECD) issued in 1981 guidelines on the protection of privacy and transborder data flows of personal data (OECD, 1981). Such regulations and the basis of such regulations are complex and difficult (TDF News, 1979, p. 1). One might ask, e.g., what legal and privacy guarantees an individual has when an ever-increasing amount of information on that individual is being stored in computer banks? What rights and protections does an individual have to correct false or misleading information collected on this individual? The situation becomes even more difficult when such computerized information is collected in one country, transmitted via a private telecommunications network owned by a corporation in another country, processed in a third country, and possibly stored in yet a fourth country. It is questionable if domestic privacy protection laws and safeguards still are operative once the data have crossed a border. What legal course of action should or could be taken? What sort of regulation and legal entities, if any, should exist at the international level? Liability in TDF is a complex issue and some have suggested that an International High Data Tribunal be created that could tackle and settle such thorny problems.

One can imagine how quickly this situation triggers discussions concerning the free flow of information, a nation's sovereignty and the right of a nation to protect its citizens from outside unwanted information. Differences with regard to philosophical, social and

cultural concerns stem largely from differences in ideologies as well as in legal principle--in some countries viewed as human rights--i.e. the right to freedom of opinion and information. The underlying assumption for such a position is a concrete form of freedom of expression and, consequently, free dissemination of information and ideas. Other countries, above all, Eastern Europe, place greater importance on the right of states to protect their national sovereignty together with their social, cultural and political values (Wigand, 1982; Hamelink, 1979). As an Academy for Educational Development report concluded: "Implications for the future may include a redefinition of national sovereignty that extends beyond traditional notions of geographical or spatial sovereignty and into 'informational sovereignty'" (Academy for Educational Development, 1978, p. 100).

Social Issues: Cultural

At the cultural level of society, one cause for the increase in TDF regulation is the intolerance of cultural encroachments brought about by satellite, computerized and other transmissions that utilize modes of thinking, language, or ideas unique to the culture sending data, information or programs (cf., Wigand, 1983a & 1982). Several views on this subject were presented by delegates at the 1980 Intergovernmental Bureau for Informatics (IBI) World Conference on Transborder Data Flow Policies held in Rome (Transnational Data Report, 1980b, pp. 1-2). Brazilian delegate, Joubert de Oliveira Brizida, Executive Secretary of the Special Secretariat of Informatics, stated:

> It is a fact that the information process threatens the cultural identity of peoples. Informatics is not neutral. It bears within itself the culture that produced it. The language, in its synthetic and semantic aspects, will receive extraordinary influence from the automatic retrieval systems and information services. Such an effect will be one of the results of producing information through structures of thought alien to the culture that uses it (de Oliveira, 1980, p. 33).

It is precisely this type of thinking that is motivating nations around the world to regulate and limit international data and

broadcasting traffic. Yet, at the same time, this view reflects the cooperative efforts of countries with similar cultural backgrounds in order to promote cultural integration. Even as limits are imposed, nations value the exchange of information resources as the most effective means "to strengthen the commercial, scientific, technological and cultural ties among nations" (de Oliveira, 1980, p. 32). It would seem that rewards would be high from a cultural standpoint if cohesive international agreements could be reached on TDF issues. Unfortunately, issues of "cultural sovereignty" often act to prevent this accord. Part of the problem lies in the vested interest of some TDF participants in the free flow of information, regardless of effect on different cultures. Some European countries feel uncomfortably reliant on U.S. American information banks (e.g., the use of the New York Times Information Service Data Base) which provide only an American point of view (Sanger, 1981). But on the other side of the cultural sovereignty coin is simply the lack of awareness of the importance of autonomy and diversity to many cultures.

Presenting his views in a report to the IBI conference, Morris H. Crawford, past Executive Director of the U.S. Interagency Task Force on TDF, made the following comment:

> 'Cultural sovereignty' was the transborder data area that Americans had most difficulty in comprehending, perhaps because 'the melting pot of the world' idealizes cultural adulteration and produces an unconscious intolerance for those who do not accept it. ...The U.S. concept of free flow of information is accepted by no one else. A more practical formulation by the U.S. is long overdue (Crawford, 1980, p. 39).

R.V. Austin, Unilever representative at the IBI conference, attempted to defend industry's need to conduct business efficiently and competitively. He said that business was "the goose that lays the golden egg--that golden egg that pays for your roads, schools, hospitals, radio stations and data networks." Austin claimed that Unilever was organized to "be sensitive to national characteristics and local conditions," and promoted the view that cultural exchange is

inevitable and desirable, as "culture is an organic thing ... enriched by change and cross-fertilization (Austin, 1980, p. 20)." Crawford (1980) also defended the necessity of some transfer of technology, but, on the other hand, called for a more precise and reasonable delineation of the acceptable parameters of cultural influence.

Another culture-related issue of TDF is that methods of regulation are widely divergent among various cultures, causing confusion and difficulty in compliance (Wigand, 1983a). One view on this topic was presented in an IBI conference address by Christian D'Aumale, French Ambassador to OECD. He raised questions on the advantages and disadvantages of this diversification of solutions to international information regulation. On the one hand, he stated, diversification would allow the adoption of informatics to fit social and cultural differences. On the other hand, he asked whether too much diversity might lead in the long run to the "incapacity to master certain aspects of questions of interest to all mankind." Thus, while he favored growth of independence, autonomy of nations, and diversity of human societies, D'Aumale did not condone a babel of tongues on international TDF regulation (D'Aumale, 1980, p. 29). Also not to be glossed over is the extra financial and operative strain placed on transnational corporations when international regulations are diverse (Hirsch, 1979).

Considerable concern has been expressed about TDF and its effect on developing countries. Such flow of information can demonstrate quite poignantly the considerable difference between information rich or data rich and information poor or data poor countries. Schiller (1978, p. 192) pointed out that such one-sided developments can further widen the communication gap within developing countries. In part, he argues, the new computer-telecommunications technologies are to blame for the creation of elite classes in these countries. Developing countries also tend to fear that when large data banks of information are "homogenized" with the records of nationals of other nations, a nation's culture and national identity may erode (National Information Policy, 1976, p.141).

Social Issues: National

At the national level, matters of security and vulnerability rank high on the list of TDF regulatory determinants. Governments have begun to claim national information rights similar to those accorded to the individual in the Declaration of Human Rights, which protects those concerned against the abuse of personal privacy, freedom, and integrity. Charles Dalfen of the Canadian Radio-Television and Telecommunications Organization states that these rights are threatened when:

> Vital data bases or computer services necessary for the effective functioning of government or business are physically or technically under the control of foreign authorities, and subject to the political decisions, technical breakdowns, labor unrest or other vagaries in those jurisdictions (Dalfen, 1980, p. 5).

This concern is augmented when governments express their unwillingness to allow continued exploitation of national information resources, such as data on natural resources or agricultural yields secured by remote sensing. The expatriation of national information often results in decisions being made outside a country on matters of that country's development or growth. Understandably, governments may choose to limit such data flow if they want to maintain control of the economic development of their states or nations. In Canada, for instance, government leaders are concerned about the vast quantity of data being exported for processing. As Peter Robinson of the Canadian Department of Communications said:

> For industrialized countries, a major part of the data flowing across international borders relates to data transfer between subsidiaries in one country and headquarters in another. In this situation, data are transferred for storage as well as processing at the headquarters facility. For Canada, this amounts to some 90 percent of the data exported for processing. It is this large net outflow of data for processing and storage abroad that is the cause of concern, for the country where the data are processed and stored tends to be the location where decisions are made (Robinson, 1980, p. 18).

Robinson's view is echoed by many others in both industrialized and developing nations. In Brazil, this view is seen to justify

control of access to strategic information resources. Policy is being implemented to eliminate the "geographic separation between the decision-making process and the productive process," also to avoid the "risk of becoming intolerably dependent, through telecommunications, on the interests of political and economic groups [who are] outside its borders and usually unconcerned about the legitimate desires of its people" (de Oliveira, 1980, p. 33).

Social Issues: International

This dependency also occurs in areas of information trade other than those of corporate interest. For example, in 1979, 63 percent of scientific and technological bibliographies were based in the U.S. (by volume of activity), and a high degree of dependence on these was evidenced by those European countries, particularly in areas of medicine and chemistry (Information Systems, 1979, p. 9 & Lemoine, 1979, p. 6). Now, however, changes occurring at the international level of society may allow for a lessening of such dependence.

EURONET, for example, established by the European Economic Community (EEC) in 1979, provides access to over 30 scientific and technical data bank and telecommunications network services at uniform, minimal cost throughout the EEC. Besides developing data banks for Europe that were previously only available in the U.S., EURONET's objective is to provide data communication services for as many potential users in Europe as possible. This is accomplished by the provision of international interconnected access from various national networks, such as TRANSPAC in France, PSS in Great Britain, and IDN in West Germany (Gresser, 1979).

Thus, at the international level, social forces for change exist not only for personal privacy protection, but also for controlled growth of the international information industry. Regulation of international privacy protection has grown to the point where it has become a political/legal issue of major concern. These developments and trends will be addressed later. But regarding the control of TDF

growth, it is possible to speculate that should regional or cultural groups of nations prove successful in utilizing the synergy of their combined efforts to develop information trade, the rise of protectionism on the part of individual nations may be partially countered. Such cooperative effort may also minimize dominance of transnational corporations as viable competition arises to help fill the void in technological achievement of some nations. The degree of success attained by EURONET and other regional networks may be an indicator of the chances for balancing national independence with worldwide interdependency.

Economic Issues: Information as Commodity

As developing nations struggle to effectively utilize and adapt to information age technology, economic issues enter the forefront of TDF regulatory considerations. These issues center around three concerns: (1) treatment of information as a commodity; (2) the threat of TDF to developing countries' balance of trade, employment, and infant information industries; and (3) restriction of competition and market entry of transnational corporations in developing nations due to tariffs, prohibitive pricing, and other impediments, including monitoring and other enforcements of privacy legislation.

The first of these issues, the treatment of information as a commodity, has its basis in the exponential growth rate of information traffic and related services. Is information actually becoming a commodity? A recent Department of Commerce report claimed that more than 50 percent of the GNP in the U.S. is comprised of data transmitting, gathering, and handling industries (Longsworth, 1980). According to Porat (1978, p. 4):

> In 1967, 25.1 percent of the U.S. Gross National Product (GNP) originated with the production, processing, and distribution of information goods and services sold on markets. In addition, the purely informational requirements of planning, coordinating, and managing the rest of the economy generated 21.1 percent of GNP. These informational activities engaged more than 46 percent of the work force, which earned over 53 percent of all labor income. On the strength of these findings, we call ours an "information economy."

Information retrieval services, just one segment of the computer services market, have increased considerably in the United States: total domestic revenues increased from about $2 billion in 1970 to $8 billion in 1978. International revenues enjoyed an increase from about $300 million in 1972 to $800 million in 1978 (United Nations Centre on Transnational Corporations, 1981). Currently, it is estimated that "the world on-line data base market, excluding those data bases not publicly available, range from $1.5 to $2 billion" (Transnational Data Report, 1982a, p. 341). During the last twenty years private telecommunications and computer service networks have enjoyed an astounding growth. Read (1977) writes that by the early 1970s private service networks accounted for one-third of all U.S. international telecommunication revenues. Silverman (1978, p. 28) states that:

> Within the international telecommunications industry, it is almost axiomatic that international services represent a growth industry. Forecasts abound projecting the explosive growth of international data services and the continued development of traditional markets for international services during the next decade.

In 1975, and growing by 20 percent annually, transmission and computer service revenues of nearly $1 billion were derived by U.S. firms from European sources alone (U.S. Department of State, 1977). This $1 billion is only a small part of information-related earnings, as no estimates are included for general industry TDF (i.e. airlines, auto manufacturers, bank and finance corporations, hotels, and major trade associations). Included in these data are, however, figures generated by common carriers providing transmission services, and independent and manufacturer service bureaus selling software, or data base and processing services. The projected on-line data base service market alone for 1985 is over $4 billion, with an average annual growth rate estimated at 24 percent (INPUT, 1980). Thus, it may be seen that information-derived revenues are an increasingly important factor of the economy.

Some view information as a commodity and use this perception to

make a case for regulating TDF just as other commodities are regulated. Morris Crawford (1980, p. 39) states that information may be thought of as being on "a continuum ranging from raw data to finished information," with value added at various points along the way. Under this model, information could then be taxed as are other value-added products. British computerized data base services, i.e. Prestel, are currently taxed in this way at a 15 percent value-added rate. But research must be conducted to determine whether information should be taxed differently than material commodities, especially since many data and information flows are not marketed in a manner conducive to interpretation of value-added status. Thus, regulation of TDF may well be affected in the future by the value of information as perceived by tax authorities.

But it is not easy to assign value to ideas, or even to determine ownership, even though information can be very expensive to produce. The number of hours and other resources that go into research, for example, are often not reflected in the sale price of information. This may be due in part to the ease of copying information, but a seller of information may either continue to possess a valuable commodity after it is sold, or he may find it valueless once it has served its purpose (Sanger, 1981, p. 8). Information as an "economic good" conflicts with views of information as a "public good," for the former requires fixing of prices to cover costs, while the latter connotes free trade and accessibility, as in public libraries.

Some argue that "free" international trade of information should be limited, at least temporarily. Just as was true of post-war material goods industries in Europe and Japan, the information industry will require time, space, and economic leeway or advantage in order to develop in many nations. Robinson (1980, p. 19) states:

> We have had many years of experience in international trade in tangible goods, yet we have still not achieved total free trade in that area. Is it then reasonable to expect a total free trade in these intangibles at the outset, before we even understand the possible implications?

Other factors in the information-as-commodity issue are the characteristics of the traffic or trade of international data flows. Philippe Lemoine (1979) isolates four criteria for the analysis of these flows: (1) The nature of the data transmitted, (2) the physical means of transmission, (3) the type of network user, and (4) the direction and quantity of the information exchange. This last factor is a primary cause of contention because of its important effect on international balances of trade and employment levels. Lemoine claims that "information traffic is all one way and shows an increasing European and Canadian dependence on the United States" (p. 4). Similarly, others argue in favor of a "free and balanced flow" of information, rather than "free flow," which may create dependence (Transnational Data Report, 1980b, p. 2).

Economic Issues: Information Trade, Employment, and Industries

The second major economic concern, then, involves limiting of TDF to enhance this balanced flow and to aid development of information trade industries, such as data processing and data base or network services, and to promote favorable international balances of trade and levels of employment. The leader of the debate on these issues is Canada, who defends her need to protect the above-named economic integrants from adverse affects of out-of-country data processing. Regarding the balance of trade, Robinson (1980, p. 8) estimates his country's imports of remote processing and data storage services will amount to $1.5 billion by 1985. As imports increase, the job market also suffers, and Robinson predicts Canada could lose up to 25,000 data processing jobs by 1985 and up to four times as many supporting function positions (management, clerical, office, etc.). Here, ultimately, is the most salient reason given in defense of TDF controls. Nations feel they must protect development of information trade industries. As automation increasingly displaces workers, information-age industries may become significant in providing jobs to fill the employment gap in the long run.

There are a host of reasons why transnational corporations have created transnational computer-telecommunication systems. The most obvious reason is the notion of control. Transnational corporations are complex creations striving toward integrated, efficient global operations. Management in such a setting is in many ways remote-management of widely-dispersed subsidiaries around the globe. A vast amount of information is needed to control, manage and monitor such an organization. The information needed may vary from subsidiary to subsidiary due to product differences, different distribution systems, different markets, and considerable variations in fiscal, political, economic, and legal environments. In addition, it may be necessary that the gathered, stored or processed information is transmitted quickly and it may have to be updated continually. Often such information has to be available on an on-line basis around-the-clock: data and information available through reservation systems, inventory control, credit authorization and the like cannot wait for an over-night update (Wigand, 1981).

The international business environment has changed since the 1950s and 1960s also. International business is no longer stable and predictable. Prices, values, interest and exchange rates can change drastically within just one hour. For corporations wanting to take advantage of business opportunities in this environment and in an effort to minimize losses and risks, speed, on-line access and integration of information systems and networks are the prerequisites. Given this setting, the development of transborder data flow as it is known today was a quite natural development. Such computer-telecommunications networks allow the transnational corporation to make instant decisions and to allocate their resources accordingly.

Aside from the control and management use of transborder networks, numerous other applications exist: R & D activities, customer services, buyer questions, market research, product planning and coordination, accounting, financial and budgetary control. Other advantages of such networks can be recognized in economies of scale

(e.g., using one central mainframe computer for processing rather than duplicating this effort at each subsidiary), and in the worldwide standardization of numerous activities.

In some of the information-intensive industries alluded to earlier, it has become mandatory to develop closed user-group transnational networks. These are computer-communication systems that service the needs of their subscribers for interorganizational transborder data flow. Three examples of the closed user-group networks are Eurex, SWIFT and SITA. Eurex, SA. and the Society for Worldwide Interbank Financial Telecommunication (SWIFT) serve numerous financial institutions. The Societé Internationale pour la Télécommunication Aeronautique (SITA) serves the worldwide air transport community.

Economic Issues: Restriction of TNC Competition

The third area of economic concern involves the use of legislative and non-legislative barriers to the free flow of transnational corporate TDF. In the non-legislative category there are tariffs, discriminatory pricing, and hard-to-meet technical standards. American business executives have attested to these before the U.S. Congress (U.S. Congress, 1980). The Office of the U.S. Trade Representative prepares lists of such trade barriers in 31 countries, ranging from "restrictions on the availability of leased lines," to "import controls," "excessive tariffs," and "government subsidy" or "support of data processing industry" (Transnational Data Report, 1982b, pp. 179-185).

From another perspective, the Commission of the European Communities (Commission) and the European Parliament have addressed specific issues of transborder data flow and the general topic of information technology and its impact on the economy and society. While the European Parliament (1979) prepared a report concerning individual rights and data processing, perhaps the most significant effort undertaken by the European Community involves its proposals for

a unified Community approach to the development of the data processing and communications industries, for the effective utilization of these information resources, and for the protection of European markets.

The development of EURONET, the community-wide communications network, is one concrete example of European Community efforts to establish a common European approach to developing new technologies. Those efforts also reflect an apparent determination to create a dominant, Community-wide carrier in the European data communications market. Indeed, American data base providers have already voiced their fears. McGraw-Hill, parent company of Data Resources, Inc., described the problem for U.S. vendors:

> The highly discriminatory tariffs that would result if American companies, even those with computers in Europe, were forced to use high, volume-sensitive rates of the PTT common carriers while European competitors had access to the far cheaper and doubtless far more efficient EURONET services would constitute an almost insuperable and wholly unjustified barrier to competition (U.S. Congress, 1980, p. 35).

But arousing the most controversy are the effects of legislated enforcement of TDF trade law. Often required is monitoring of once-secret company data by Data Protection Agencies (DPAs), a policy instituted by some nations to ensure compliance with the law. TNCs believe monitoring threatens their competitive viability, as data and methods of doing business become open to possible surveillance by entities who may not have the company's best interests in mind. Presumably these entities might include the competition, which in some cases is represented, sponsored, or comprised by the government itself.

Legislated and non-legislated barriers are manifestations of a recent trend toward protectionism, in the view of first-world TNCs, who are complaining about the new threats to their competitive abilities. The U.S. government responded by calling for a convention of GATT (General Agreement on Tariffs and Trade) members last year, in which the U.S. intended to work towards a reduction of protectionism. At the convention, in November of 1982, such intentions met with little success, due in large part to the worldwide recession. The

only concession that ministers would make in regard to data processing was to "... look at the rising trade in international services ... and to decide later whether to draft new agreements for the free flow of such activities." Trade in services was established "as the next target for liberalization later this decade ..."(Farnsworth, 1982). France, on the other hand, hopes to amend GATT so that taxes may be charged on the retail value of software (Sanger, 1983, p. 26F).

Thus, technical, social, and economic concerns may be seen to be significant causes and indicators of TDF regulatory trends. The political and legal circumstances of existing and proposed TDF regulation reveal the measurable realities of the international situation. In the following section, research findings are described from the authors' analysis of national and international data and privacy protection policies. A total of 22 nations was identified whose governments have already enacted or are now considering TDF regulation.

Political/Legal Issues and Current Situation

The first area of transborder data flow to come under the scrutiny of national regulators was the issue of personal privacy. Electronic data processing greatly increased the ability of data bank operators to collect, process and disseminate personal information. The ability to control more information about an individual than was necessary could and did lead to abuses of natural persons' rights to control their own lives. Some nations have had laws on record for hundreds of years that, to a certain extent, protected information on individuals from exploitation.

Sweden was the first country to enact legislation specifically controlling the automated use of personal data. The Swedish Data Act of 1973 licensed public and private organizations that maintain registers of persons. This precedential legislation set the stage for a flood of similar laws in most of the non-communist industrialized nations. An examination of the major issues of enacted regulation

should provide businesses, social scientists and legislators an insight into the way privacy regulation has been developed and how it provides a platform from which to judge and implement future legislation. Data on privacy regulation in 22 nations have been compiled by these authors and will be examined issue by issue (cf., Table I).

Protected Persons. The first specific area of concern of privacy legislation is the scope of coverage. As indicated in Table 1, natural persons are protected by most of the nations that have privacy legislation. An alien's right to protection is not always guaranteed and some countries, such as Canada, only afford protection to their citizens. The major area of difference in the coverage granted lies in the rights of legal persons. A "legal person" is a corporation or company granted the privileges, legal powers, liability and rights of an individual (natural person). When a country extends privacy protection to both natural persons and legal persons, it exceeds international agreements, such as OECD guidelines, which only seek to control data on natural persons. Norway included legal persons because of the difficulty of separating entrepreneurs' credit information from that of their companies. In countries where small business undertakings play an important economic role, it is difficult to distinguish how best to protect the entrepreneur's privacy. Norway regulates data on legal persons in the private sector, but not in the public sector.

Name-linked Data. Once it has been determined who is covered by privacy regulation, it must be established what is covered. The most commonly used method of identifying data capable of being abused is to see if the data are name-linked. This means that any data indexed by an individual's or legal person's name or related identification number, depending on their sensitivity, could fall within the sanction of privacy regulation. Countries such as Denmark apply their laws to other types of systematic registration, which would include personal

files organized by subject or date. Personal data are defined by the Council of Europe as "any information relating to an identified or identifiable individual," or "data subject"" (Transnational Data Report, 1980a, p. 17). The common denominator here is the potential damage or exploitation that could result if information were abused.

Most information that is commonly available, such as phone numbers and addresses listed in publicly accessible books is not protected. Credit and religious affiliation information contained in data banks is generally afforded protection under most privacy laws. Konrad Stollreither (1980, pp. 9-10), Data Commissioner of the State of Bavaria, Federal Republic of Germany, uses five levels of non-binding classifications of personal data systems. An abbreviated look at these categories readily shows the complexity of potential personal information abuse:

Level of protection A: Freely accessible data. The user of such data is not obliged to prove a lawful interest in the data. Examples: directories, telephone books, published lists of membership.

Level of protection B: Data which if misused do not significantly harm personal interests. These data are not freely accessible. Their use is restricted to authorized interest. Examples: title, academic degree, description of profession, business or classified directory information, bank connection, payments for utilities.

Level of protection C: Data whose misuse can harm the person concerned or his reputation. Examples: marital status, religion, nationality, military service, school reports, employment, income, memberships, traffic tickets.

Level of protection D: Data whose misuse can significantly harm the person concerned in his reputation or his economic interest. Examples: Condition of health, conviction to an asylum, criminal convictions, professional references, financial status, assets, debts, bankruptcies.

Level of protection E: Data whose misuse can injure the health, life or freedom of the person concerned. Examples: Extremely sensitive data of patients, data of persons who possibly could be victims of criminal actions, such as the protection of witnesses.

Name-linked data can be processed and manipulated in both manual (MDP) and automated or electronic data processing (ADP or EDP)

Table I: Transborder Data Flow, Data Protection and Privacy Regulation in 22 Nations

PERSONAL PRIVACY REGULATIONS & ISSUES	COUNTRY	AUSTRALIA	AUSTRIA	BELGIUM	CANADA	DENMARK	FINLAND	FRANCE	HUNGARY	ICELAND	ISRAEL	JAPAN	LUXEMBOURG	NETHERLANDS	NEW ZEALAND	NORWAY	PORTUGAL	SPAIN	SWEDEN	SWITZERLAND	UNITED KINGDOM	UNITED STATES	WEST GERMANY	EEC [1]	COE [2]	OECD [3]	IBI [4]
A TYPE OF REGULATION*,**		LP	L	LP	L	L	LP	L	LP	L	L	R	L	LP	L	L	LP	LP	L	LP	R	L	L	R	R	G	R
B. PROTECTED PERSONS - Natural Persons		X	X	X	X	X	X	X			X		X	X	X	X		X	X		X	X	X	X	X	X	
Citizens/Residents Only					X																	X					
Legal Persons			X	X		X							X		X	X									X		
C. NAME-LINKED DATA --EDP/ADP		X	X	X	X	X	X	X			X		X	X	X	X		X	X		X	X	X		X		
Manual Data Processing		X	X		X	X		X						X		X		X				X	X		X	X	
Collection/Flows/Storage		X	X				X	X			X		X		X				X					X	X	X	
D. CONTROL - Data Control Boards			X	X	X	X		X					X	X		X		X	X		X		X				
Registration/Licensing			X	X	X			X			X		X			X			X			X	X					
E. RIGHT TO ACCESS/CHALLENGE		X	X	X	X	X		X			X		X		X	X			X			X	X		X			
Freedom of Information		X	X		X	X	X	X					X	X		X			X			X	X					
F. LEVEL OF GOVERNMENT - Local		X			X													X		X		X	X					
National		X	X	X	X	X		X		X	X		X	X	X	X	X	X	X			X	X					
International						X									X	X			X					X	X	X	X	
G. REGULATED SECTOR - Public			X	X	X	X		X					X		X	X			X			X	X	X	X			
Private			X	X		X		X					X			X			X				X	X	X			
Self-regulation							X																X					
H. ENFORCEMENT Fine								X					X									X						
Victim Compensation															X	X												
Data Confiscated/Destroyed				X									X						X									

*Legend:
LP = Legislation pending
L = Legislation in force
R = Report
G = Guidelines

Source: Transnational Data Report, 1978-1983, Vols. 1-6; EEC, COE, IBI Reports, OECD Guidelines, and personal correspondence.

Footnotes: [1] European Economic Community
[2] Council of Europe
[3] Organisation for Economic Co-Operation and Development
[4] Intergovernmental Bureau for Informatics

** Note that the countries studied will differ in degree of 'regulatedness' or in strength of laws and diligence of enforcement. An "X" simply denotes the existence of a condition, not its strength.

systems. Specific informational operations can be controlled through the use of privacy legislation. The variables that may be controlled include (Strollreither, 1980, p.10):

(1) control of entry
(2) exit
(3) storage
(4) user
(5) access
(6) transmission
(7) input
(8) transport
(9) organization
(10) order of process

Automated information systems may be abused more easily than manual ones. They can have greater quantities of information stored in small devices and can be accessed more quickly than manual systems. They can transmit information via land lines, microwave or satellites to terminals or data banks anywhere in the world (Wigand, 1982). MDP systems are limited in how rapidly they can be accessed and, also, transportation of manually processed and stored data is slow. MDP is treated differently in various countries. In Austria, e.g., a general right to confidentiality for all data exists, but only in regard to ADP does an individual have a right to access and challenge (cf., section on 'Right to Access/Challenge').

The manner in which information is transmitted also needs examination. Name-linked protected data, when transmitted electronically, may not be protected if they are transported manually. Data protection laws in some countries can be circumvented by mailing tapes or disks that need to be processed out of the country by air express rather than by electronically transmitting their contents.

The United States favors protection of both manual and computerized systems. When both areas, i.e. MDP and EDP, are covered by privacy regulation, abuses are limited. Countries that have the most regulation of personal data usually control the ADP area most heavily.

Control. The type of data control board or regulatory agency established to enact or monitor privacy regulation varies from country to

country. Differences depend on type of legislation and funding. Denmark has a Register Board which makes an assessment before a personal register can be formally authorized. Applicants must formulate operating instructions which are in keeping with provisions of data protection laws. Transborder data flows out of Denmark are also subject to a special export license. In some countries, boards are empowered to license all data registers that contain name-linked data. In others, not only name-linked data, but also trade or personal data that are not name-linked are controlled. Some regulating agencies have the ability to monitor data transfers or require a copy of encryption codes used in transmitting data. Sweden has an appeals branch that handles complaints and acts as an ombudsman for the rights of individuals or protected persons. In Finland the main control is from the computer industry, which has passed a non-legislated (voluntary) set of guidelines which most users treat as binding. The United States so far established laws on an issue by issue basis with judicial remedies rather than by one-piece national legislation under the jurisdiction of a single governing board. Legislative and regulatory differences have resulted in difficulties for international users of information systems. They now must unravel each country's regulatory method of privacy legislation and administrative apparatus.

Right to Access/Challenge. Under most data protection laws, individuals are granted certain rights to ascertain who has information on them, the nature of the information, and the right to challenge incorrect data. An individual's right to challenge the use of data or content of files and the ability to find out what is known about them has evolved from issues of freedom of information (FOI) and related legislation. How an individual discovers where his personal data are located depends on the degree to which data banks, both private and public, are made known and made accessible. Countries with FOI laws often require data registeries which make research easier. In countries with no FOI laws, the individual is often

dependent upon regulatory boards of government officials for monitoring personal data protection.

Levels of Governmental Regulation. Privacy legislation has been enacted at all levels of government. The State of New South Wales in Australia, e.g., has enacted privacy protection regulations. Most states in the U.S. have passed some form of privacy legislation. The apparent need for privacy protection has caused local governments to enact laws when national or international bodies were slow in formulating policy. This may provide privacy protection on a microcosmic level, but unilateral law-making in privacy legislation can defeat the ability of states or countries to have reciprocal agreements on name-linked data that cross their borders. For this reason, similarities exist in the way name-linked data has been treated in most free-world, industrialized nations.

International organizations such as the OECD have established guidelines to create multi-laterally similar privacy laws. Cooperation on privacy legislation among countries is an on-going process: Data protection commissioners from Austria, Denmark, France, Germany, Canada, Luxembourg, Norway, Finland, and Sweden meet frequently to discuss and coordinate current and future privacy needs. This type of cooperation should help to provide protection for the individual while reducing confusion about data handling. This, in time, may prevent the creation of new and insurmountable blocks to information exchange among countries in the future.

Regulated Agency: Public and Private Sectors. The vigor with which a country mandates protection of individual privacy can sometimes be ascertained by examining which agencies are required to participate in the privacy regulation. Differences may be noted between private and public sector operations. It is understandable that governments may have special regulating governing national security data. On the other hand, national security has been used for ulterior purposes in

modern history and one may want to question governmental exclusions. As an example, J.K. Williams (1982, pp. 156-157) of IBM United Kingdom Ltd. noted in a recent paper:

> Public sector files merit close scrutiny because of the sovereign nature of the power of government over the individual, the numbers of individuals covered in public sector files, the frequently detailed and sensitive nature of the data on those files, and the fact that the individual has no freedom to choose, but is usually compelled by law to disclose personal data to government agencies.

Private sector data registers are regulated to the extent that they are perceived as a threat to personal privacy. Germany employs data commissioners for the public sector but relies on self-regulation for the private sector. As indicated in Table I, most of the nations that have data control boards include private sectors. Sweden's experience in licensing private data registers exemplifies the problems encountered in regulating the private sector. Sweden's OSK Commission (Commission on Publicity and Secrecy of Official Documents) estimated that there would be 4,000 systems to be licensed, but more than 30,000 applications have been received. It was necessary for the Data Inspection Board to initiate a "short licensing" system under which 70 percent of all applications were registered without the lengthier approval system originally conceived when the legislation was initiated. Sweden's population is 8.2 million. By comparison, in countries such as the United States where the population is many times greater and information processing constitutes a significant percentage of the GNP, the cost of licensing and administration could be staggering. The problem is greatly exacerbated by the fact that many data registers are used for multiple applications, and it is conceivable that many licenses would be needed by a single data register. When licensing requirements are ponderous, participants must evaluate and contend with the cost of compliance. It is in a nation's best interest to have realistic licensing requirements.

Enforcement. In countries where licensing laws are in effect, the threat to a firm of losing a license, once it had been granted, is a

deterent to misuse of data. Combinations of fines, victim compensation and data confiscation have also been legislated. In Belgium, violators of privacy legislation are libel for a maximum prison sentence of two years, and the abused data are subject to destruction. In France, the maximum sentence is five years imprisonment, a fine of 2 million Francs, and publicity. Norway's criminal penalties are one year in prison and the victim of the breach of privacy is compensated. A data board in Canada reviews complaints and investigates charges to see which are valid. Actual privacy breaches are corrected. Due to the newness of personal privacy legislation few precedents have been established on how best to control violators. Guidelines provided by the Council of Europe (Transnational Data Report, 1980a, p. 17) in Article 10, "Sanctions and Remedies," require that "each party undertakes to establish appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection ...." As nations develop experience with privacy violation, penalties will be established that are in keeping with the crimes.

Other Considerations. Further examination of Table I underlines the concern of some non-communist industrialized nations in regard to protecting personal privacy. Data from a survey of attendees at the 1978 IEI sponsored Strategies and Policies in Informatics (SPIN) conference indicated that 28 countries are regulating or plan to regulate personal privacy. Forty-one countries are planning on some type of control to avoid negative social effects of pervasive computer use (Transnational Data Report, 1978, p. 11). Difficulties have arisen in trying to balance a government's sovereign rights, needs and expectations with those of business and social scientists. Issues have been dealt with in an ad hoc manner with each new piece of national legislation benefitting from insight into successes and failures of preceding data protection laws.

Impact of Transborder Data Flow Regulation

Widespread data and privacy protection regulation could impact many areas of transnational corporations' operating practices. In a study entitled, The London Meeting of the Brussels Mandate: Summary Report and Findings (1978, pp. 23-24), one corporate spokesperson presented his concern about impacts of such regulation on the user community. These include "licensing; registration of computer data bases, processing units, and associated reporting costs;" and "response to inquiries ... concerning the existence and content of data." Variations in regulatory methods may also cause problems, he continued, as "compliance with regulation in country A may cause a violation or a host of violations in country B," and "unknown, but in all probability higher, operating costs [may be] incurred for system redesigns which may be necessary on a country-by-country basis." Other costs might be incurred from "inspection; disclosure;" and "social responsibility;" as well as from "data taxes" and "data barriers." He concluded that there could be "a potentially significant impact on our P&Ls (profit and loss statements)," as well as on continued use and development of "electronic mail, word processing and technical optimization of our technical support systems ..."

Timothy G. Donovan (1981, pp. 27-28) indicated more specifically where impacts would be felt from regulation of transborder data flow:

- Highly-centralized systems are going to be the most affected by all forms of data flow barriers.
- Barriers imposed by PTT regulations will affect all MNCs whether they operate a private network or use some form of common carriers.
- Companies using a lot of name-linked data and who are moving it across borders will be subject to close scrutiny.
- Corporations currently holding name-linked data in countries without privacy laws might well be forced to relocate such data to countries with a generally accepted form of data protection legislation.

- Companies moving data across borders merely for data processing purposes may find those data subject to some form of taxation or
other restrictive mechanism.
- Service companies handling data which may be judged as being of a national strategic nature may, at best, have to become more 'accountable' for the use and security of the data.

But just as regulations multiply and act to restrict transborder data flow, other factors work to diminish the impact of the regulatory trend. Not yet documented, but certainly present, is the creation of so-called data sanctuaries, data havens, or data collection/processing free ports in response to national data protection laws in nations without such laws, just as Switzerland has evolved into a financial sanctuary. Electronically it is possible to collect data in a nation despite data protection laws. No enforcement means exist presently for governments to prevent information from moving across a border when this occurs electronically via existing technology. Our laws, conventional practices and the entire notion of sovereignty may be unrealistic or antiquated when we consider how information can be accessed, stored, collected and transmitted today.

Conclusion

The scope of international legislation on transborder data flows may seem excessive to those hoping to utilize or profit by international flows of data, especially data with potential for compromising personal privacy. To others, who may wish to improve privacy protection in their countries, or perhaps hope to use the legislation as a barrier to protect fledgling information economies, the current scope of legislation may seem minimal. But the actuality of the proliferation of TDF legislation may only provide fodder for heated discussions as to its impact and effectiveness. Currently there is little evidence as to whether existing laws have hampered flows of data, enhanced the privacy of individuals, or increased the sovereignty of nations. Further investigation is needed.

What is apparent, however, is that the feasibility and expense of implementing or enforcing these laws and monitoring flows of data may be prohibitive to countries that lack exceptionally abundant resources and sophisticated technology and expertise. For those who still feel that more legislation is necessary to ensure some societal good, it may eventually be found that only the joint efforts of assemblies of nations will be able to effectively regulate international flows of data. Individual nations may be finding that the broader the scope of the sectors they wish to regulate (i.e. natural/legal persons, private/public sectors), the more unmanageable the implementation and enforcement. Nations working together can overcome some of these problems by harmonizing laws to ease the task of compliance. On the other hand, international guidelines thus far have tended to seem innocuous. Often they must be developed to satisfy the demands of diverse interests at the same time as they strive to arouse the least amount of controversy possible, from business or other users of TDF. The result is that international guidelines often represent the lowest common denominator of acceptability to participating nations.

It is doubtful that such systems of negotiation and compromise will achieve sufficient agreement multi-laterally to formulate superior policy. Perhaps cooperation among economically or politically similar nations would be more expedient and successful. In any case, lengthy processes of negotiation, trial, error, and revision seem endemic to regulatory efforts. Meanwhile, the rate of change and growth of technological innovation in informatics far exceeds the speed with which legislators can react to each new threat to societal values. The question each nation must face is whether it will allow technology-driven, market-driven, or policy-driven futures (Cf., Dordick, Bradley, and Nanus, 1981). Then each nation should attempt to pursue that course of action which is in keeping with national values and goals, as well as with its relationships with the world community. As technological innovations such as personal computers and electronic mail continue to evolve and advance into common, soon worldwide usage, privacy issues and personal data use regulation will become more complex. Legislators in all nations must remain aware of the changing environment and strive to balance the need for a free flow of information with other needs for personal and national protection and benefit.

REFERENCES

Academy for Educat onal Development. The United States and the Debate on the World Information Order. Washington, D.C.: Academy for Educational Development, 1978.

Austin, R.V. Unilever's Data Flow Requirements. Transnational Data Report, 1980, 3(3-4), 19-20.

Barram, V.S. How Privacy Relates to Freedom of Information. Transnational Data Report, 1981, 4(6), 25-26.

Burnham, David, U.S. Is Worried by World Efforts to Curtail Flow of Information. New York Times, February 26, 1978, p. 1 ff.

Commission of the European Communities. European Society Faced with the Challenge of New Information Technologies: A Community Response. Brussels: European Economic Community, 1979.

Commission of the European Communities. "Proposal for a Council Regulation (EEC) Concerning Community Actions in the Field of Microelectronics," COM(80) 421 final (Brussels, 1 September 1980); "Recommendations on Telecommunications," COM(80) 422 final (Brussels, 1 September 1980); "New Information Technologies," COM(80) 513 final (Brussels, 1 September 1980).

Crawford, M.H. The IBI Transborder Data Flow Conference: An American View. Transnational Data Report, 1980, 3(3-4), 38-41.

Dalfen, Charles M. Examining Unresolved Data Flow Issues. Transnational Data Report, 1980, 3(3-4), 5-7.

(Datamation.) Canada's Economic Concerns. Datamation, November 1, 1978, p. 67 ff.

D'Aumale, Christian. French Address to the World Data Flow Conference. Transnational Data Report, 1980, 3(3-4), 29-31.

de Oliveira Brizida, Joubert. Official Brazilian Address on Transnational Data Flow. Transnational Data Report, 1980, 3(3-4), 32-34.

de Sola Pool, Ithiel. International Aspects of Computer Communications. Telecommunications Policy, 1978, 1(1), 33-51.

Donovan, Timothy G. Data Protection's Many Tentacles. Paper presented at the Computer Privacy and Security Symposium, Top Secrets 1981. Phoenix, AZ: Honeywell Information Systems, Inc., 1981.

Dordick, Herbert S., Helen G. Bradley, and Burt Nanus. The Emerging Network Marketplace. Norwood, NJ: Ablex Publishing Corp., 1981.

Economic and Dependency Issues Overshadow Privacy in Canadian/U.S. Data Flow Talks. Transnational Data Report, 1978, 1(5), p. 1 ff.

Eger, John M. U.S. Proposal for Progress Through Negotiations. Journal of Communication, 1979, 29(3), 124-128.

European Parliament. Report Drawn Up on Behalf of the Legal Affairs Committee on the Protection of Rights of the Individual in the Face of Technical Developments in Data Processing [1979-1980]. Eur. Parl. Doc. (No. 100/79) PE 56.386/fin., 1979.

Farnsworth, Clyde H. "A Reporter's Notebook: Behind The Scenes at the GATT Trade Talks in Geneva," and "A Shaky Bow to Free Trade." The New York Times, December 5, 1982.

Freese, Jan. The Dangers of Non-Regulation. Journal of Communication, 1979, 29(3), 135-137.

Gresser, Jean-Yves. EURONET: A Network for Europe. Systèmes d'Informatique [CII-Honeywell Bull Magazine], 1979, 30, 12-13.

Hamelink, Cees J. Informatics: Third World Call For New Order. Journal of Communication, 1979, 29(3), 144-148.

Heintz, Alden. The Dangers of Regulation. Journal of Communication, 1979, 29(3), 129-134.

Hersch, Phil. Europe's Privacy Laws - Fear of Inconsistency. Datamation, February, 1979, p. 85.

(Information Systems.) Europe/North America: A One-Way Flow. Information Systems, 1979, 30, 9.

(INPUT.) International Market Opportunities for On-line Data-base Services. INPUT, September 1980. (Cited in Transnational Data Report, 1982, 5(7), 341.)

Jacobson, Robert E. The Hidden Issues: What Kind of Order? Journal of Communication, 1979, 29(3), 149-155.

Kirchner, Jake. U.S. Data Policy to Stipulate Open Data Flow. Computerworld, February 19, 1979, p. 1 ff.

Larsson, T. Transnational Data--Regulatory Issues. Telecommunications Policy, June 1978, pp. 169-70.

Lemoine, Philippe. Transborder Data Flows. Systèmes d' Informatique [CII-Honeywell Bull Magazine], 1979b, 30, 2-11.

The London Meeting of the Brussels Mandate: Summary Report and Findings. London, June 15-16, 1978; unpublished report from The Brussels Mandate, 1742 N Street, NW, Washington, DC 20036.

Longsworth, Maury A., Jr. Rights and Transnational (Transborder) Data Flows. Computer Security and Privacy Symposium Proceedings. Phoenix, AZ: Honeywell Information Systems, Inc., 1980, pp. 27-28.

McHale, John. The Changing Information Environment. Boulder, CO: Westview Press, 1976.

Mendelsohn, Harold. Delusions of Technology. Journal of Communication, 1979, 29(3), 141-143.

National Information Policy. Report to the President of the United States, submitted by the Staff of the Domestic Council Committee on the Right of Privacy; published by the National Commission on Libraries and Information Science. Washington, DC: U.S. Government Printing Office, 1976.

Organisation for Economic Co-Operation and Development. Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Paris: CECD, 1981.

Pantages, Angeline. Europe Moves Toward Controlled Data Flow. Datamation, November 1, 1978, pp. 80-81.

Pipe, G. Russell. Council of Europe Data Privacy Draft Delayed. Computerworld, February 12, 1979, p. 21.

Pipe, G. Russell. National Policies, International Debates. Journal of Communication, 1979, 29(3), 114-123.

Pipe, G. Russell. Three Nations to Pass Privacy Laws in '79, More May Follow Suit. Computerworld, February 12, 1979, p. 20 ff.

Porat, Marc U. Communications Policy in an Information Society. In G. Robinson (Ed.), Communication for Tomorrow. New York: Praeger, 1978, p. 6.

Porat, Marc U. The Information Economy: Definition and Measurement. (Office of Telecommunications, U.S. Department of Commerce). Washington, DC: U.S. Government Printing Office, 1977.

Read, William H. Foreign Policy: The High and Low Politics of Telecommunications. In Anthony G. Oettinger, Paul J. Berman, and William H. Read (Eds.), High and Low Politics: Information Resources for the '80s. Cambridge, MA: Ballinger, 1977.

Robinson, P. Some Economic Dimensions of TDF. Transnational Data Report, 1980, 3(3-4), 18-19.

Sanger, David E. "Waging a Trade War Over Data." The New York Times, March 13, 1983, pp. 1 & 26F.

Sanger, David E. "Wire Static: Multinationals Worry As Countries Regulate Data Crossing Borders." Wall Street Journal, August 26, 1981, pp. 7-8.

Saur, Ricardo A.C. Protection Without Protectionism. Journal of Communication, 1979, 29(3), 138-140.

Schiller, Herbert I. Computer Systems: Power for Whom and for What? Journal of Communication, 1978, 28(4), 184-194.

Schmid, Gregory. Interdependence Has Its Limits. Foreign Policy, No. 21, Winter 1975-76, pp. 188-197.

Sieglerschmidt, H. European Parliament Report on Data Processing and the Rights of the Individual. Information Age, 1982, 4 (3), 170-181.

Silverman, Paul B. The Evolving Market for International Communications. Telecommunications, April 1978, pp. 25-30.

Slater, Karen. Long-Range Strategies Urged for Transborder DP. Computer Business News, March 12, 1979, p. 7.

Staply, Barry. Urgent Need for Deregulation. Telecommunications Policy, March 1979, pp. 74-76.

Stollreither, Konrad. Technical and Organizational Security for Data Protection. Transnational Data Report, 1980, 3(7), 9-10.

(Süddeutsche Zeitung). Jetzt reden alle vom Datenschutz. Süddeutsche Zeitung, 1983, 102, 23.

(TDF News.) OECD Guidelines in the Home Stretch. TDF News, 1979, 1(7), 1.

(Transnational Data Report.) Access to the International On-line Data-Base Market. Transnational Data Report, 1982a, 5(7), 340-341.

(Transnational Data Report.) Council of Europe Convention for the Protection of Individuals with Regard to Automated Processing of Personal Data. Transnational Data Report, 1980a, 3(6), 17.

(Transnational Data Report.) National Independence Dominates IBI World Data Flow Conference. Transnational Data Report, 1980b, 3(3-4), 1-2.

(Transnational Data Report.) Survey Shows 35 Countries to Regulate Data Flows. Transnational Data Report, 1978, 1(7), 11.

(Transnational Data Report.) Trade Barriers to Telecommunications, Data and Information Services. Transnational Data Report, 1982b, 5(4), 179-185.

Trubow, George B. Privacy, Policy and Computers. Paper presented to the Computer Privacy and Security Symposium, Top Secrets 1981. Phoenix, AZ: Honeywell Information Systems, Inc., April, 1981.

United Nations Centre on Transnational Corporations. Transnational Corporations and Transborder Data Flows (Report Prepared for the 7th Session of the Commission on Transnational Corporations). New York, NY: United Nations Economic and Social Council, 1981.

U.S. Congress, House of Representatives. 96th Congress, 2nd Session. Committee on Government Operations, Government Information and Individual Rights Subcommittee. International Information Flow: Forging a New Framework. Serial No. 96-1535. December 11, 1980. Washington, DC: U.S. Government Printing Office, 1980.

U.S. Department of State. Briefing Paper on Transborder Data Flows. Unpublished Report. Washington, DC: U.S. Department of State, 1977, pp. 10-11.

Wigand, Rolf T. Communication Among International Organizations. In W.E. Arnold et al. (Eds.), Organizational Communication. Dubuque, Iowa: Gorsuch Scarisbrick, 1981.

Wigand, Rolf T. Direct Satellite Broadcasting: Selected Social Implications. In M. Burgoon (Ed.), Communication Yearbook 6. Beverly Hills, CA: Sage, 1982, 250-288.

Wigand, Rolf T. Broadcast Satellites in Europe. Satellite Communications, 1983a, 7(4), 20-25.

Wigand, Rolf T. Deregulation of the U.S. Communications Industry. Media Perspektiven, 1983b, 6, forthcoming.

Wigand, Rolf T. Direct Satellite Broadcasting: Definitions and Prospects. In George Gerbner and Marsha Siefert (Eds.), World Communications: A Handbook. New York: Longman Publishers, 1983c, pp. 183-187.

Williams, J.K. European Data Protection -- A Business Viewpoint. Transnational Data Report, 1982, 5(3), 156-157.

Yurow, Jane. Privacy Legislation and the Restriction of Transborder Data Flow. Information Age, 1983, 5(1), 11-15.